CRITICAL INFRASTRUCTURE DEVELOPMENTS

October 25, 1999
Issue 16♦99

Editors: Linda Garrison
Martin Grand

Associate Editor: Brenda L. Jones

! Internet Commerce: Best Practices Combined with Current Internet Security Tools Can Deter Electronic Fraud and Deception

! NIPC Information Systems Advisory 99-024: RingZero Trojan Program

This publication provides information on current critical infrastructure protection issues, with emphasis on computer and network security matters.

This issue has an overall classification of “Unclassified."

Analytical commentary within is identified in **bold** text.

We welcome your comments and suggestions for improving this product. For more information, or to provide comments, please contact the NIPC Watch at **nipc.watch@fbi.gov** or call (202) 324-0334 or (202) 324-0353.

Internet Commerce: Best Practices Combined with Current Internet Security Tools Can Deter Electronic Fraud and Deception

Security breaches in the electronic commerce arena could be reduced or avoided by increasing user awareness and the implementation of new security tools.

Currently, the safe transmission of Internet commerce relies heavily upon, but is not limited to, security standards and protocols, sophisticated encryption algorithms, and system administrator support. The complexities associated with these security technologies can often create a false sense of security for many non-technical Internet users, and can create an opportunity for electronic fraud and deception. Widely-accepted security standards such as the Secure Socket Layer (SSL) are a vital security component, but these standards are not the complete solution to conducting secure transactions via the Internet. Internet intrusion incidents have exploited the average user=s false expectations and lack of technical expertise by using simple, deception strategies that have resulted in problems such as the compromise of users= passwords, account information, and loss of funds. Furthermore, the likelihood of intruders exploiting these same vulnerabilities and repeating similar intrusion tactics in the future is very high.

A variety of Internet intrusion incidents have evolved from a commonly-known Internet vulnerability: the intruder=s ability to redirect a user to a replicated or different Internet site. The redirected site is often identical to the user=s originally-requested site, which can lead to the user unknowingly entering his or her username and password(s) into the pseudo site. In 1997, Eugene Kashpureff of Canada successfully deceived thousands of Internet users by redirecting their Internet address requests to his specified Internet address. He accomplished this by gaining access to a vital control point (Domain Name System, or DNS) which allowed him to covertly redirect anyone requesting the targeted Internet address. A different but more recent example involves a major Internet Service Provider (ISP), whose members received email prize advertisements that contained pseudo links. The ISP user clicked on the pseudo link and connected to a replicated ISP home page which asked for the member=s username and password. Numerous subscribers were fooled by the replicated home page, and voluntarily gave their personal information to the intruder(s). Another likely scenario would be if an intruder were to gain access to a DNS control point that directed activity for an Internet transaction site. The intruder would then redirect an unwitting user to an exact replica of the requested site. If fooled, the user would enter his or her username and password. The intruder would capture the password and have complete access to the user=s account and could use the account for fraudulent purposes. To bolster the deception, the intruder could redirect the user back to the original authentic site, thereby leaving the average user to believe that his or her last access attempt had simply been unsuccessful, with no idea that their account had just been compromised.

Widespread misunderstanding of the abilities of security technology, combined with the known exploitation of Internet transaction vulnerabilities by intruders, creates the potential to exploit future Internet related commerce. New security technologies such as the Secure Electronic Transaction (SET) system, the Transport Layer Security (TLS)

system, and a proposed transaction security technology by Digital Bond, Inc. will help prevent future intrusion incidents. Moreover, the combination of new security technology, coupled with increases in user awareness of the potential for electronic fraud, will help deter redirection intrusion attempts.

NIPC Information Systems Advisory 99-024: RingZero Trojan Program

RingZero demonstrates a new, aggressive reconnaissance technique that is currently being used to map target systems and could be used to support malicious activities.

As reported by the SANS Institute, large numbers of government and commercial sites have experienced an unusual volume of network scans from multiple origins in the past two months. This activity involves a Windows-based Trojan horse program called RingZero that is designed to infect client machines without the user's knowledge. This Trojan appears to be a remote-controlled, distributed scanning engine that is configured to scan ports 80 (common port for World Wide Web), 8080 (common port for World Wide Web proxy services), and 3128 (common squid proxy services). Its origins are currently unknown, but unconfirmed reports indicate that it was distributed initially via e-mail, possibly with another program such as a screen saver or game.

In the estimation of John Green of the Naval Surface Warfare Center, this wide-spread Internet scanning reflects a significant advance in "distributed attack technology" because of RingZero's transmission rate; dynamic configuration options (may be able to go from scanning to attacking); and automated result consolidation.   RingZero Trojan might be used for:

- Coordinated mapping of networks for future attacks.
- Attempting to locate computers running proxy servers because of known proxy vulnerabilities.
- Attempting to locate proxy servers running outside of a misconfigured firewall as a tool to gain access through the firewall.
- Relaying and anonymizing large distributed cgi-bin attacks.

The NIPC recommends using the information published in the System Administration, Networking and Security (SANS) Institute Flash Advisory (located on their Web site at: <http://www.sans.org/newlook/resources/ringzero.htm>) to block unneeded services as a defense against the RingZero trojan. If services on ports 80, 8080, and 3128 are used, system administrators personnel should examine outbound traffic originating from these ports that are directed to unknown or suspicious sites. The NIPC strongly recommends that activity of this nature be reported to appropriate computer emergency response organizations, information technology security organizations, or the NIPC.